

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2003174443 A**

(43) Date of publication of application: **20.06.03**

(51) Int. Cl.

H04L 9/08
G06F 15/00
G06F 17/60
H04L 9/32

(21) Application number: **2001373674**

(22) Date of filing: **07.12.01**

(71) Applicant: **SONY CORP**

(72) Inventor: **ISHII HIDEHIRO**

(54) INFORMATION PROCESSOR AND INFORMATION PROCESSING METHOD, PROGRAM STORAGE MEDIUM, AND PROGRAM

(57) Abstract:

PROBLEM TO BE SOLVED: To freely deliver and distribute contents, and to flexibly set a license for using the contents.

SOLUTION: A contents server encrypts contents in providing the contents via the Internet to a client. Then, attribute information associated with the contents is described in the header of the encrypted contents. The client acquires a license to permit the encrypted contents by performing an access to a license server to acquire a license where the attribute information of the contents fulfills an attribute condition.

COPYRIGHT: (C)2003,JPO

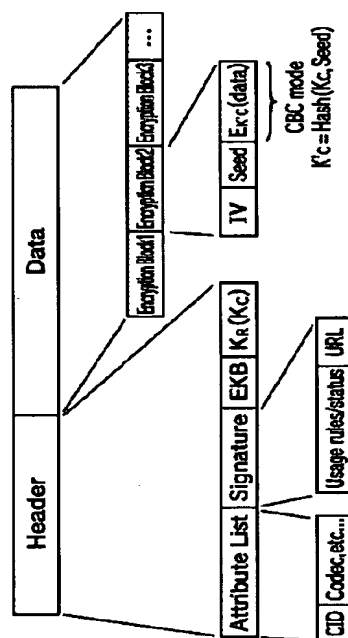


FIG. 5

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2003-174443
(P2003-174443A)

(43) 公開日 平成15年6月20日 (2003.6.20)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
H 0 4 L 9/08		G 0 6 F 15/00	3 3 0 Z 5 B 0 8 5
G 0 6 F 15/00	3 3 0	17/60	1 4 2 5 J 1 0 4
17/60	1 4 2		3 0 2 E
	3 0 2	H 0 4 L 9/00	6 0 1 B
H 0 4 L 9/32			6 7 3 Z
審査請求 有 請求項の数11 O L (全 18 頁)			

(21) 出願番号 特願2001-373674(P2001-373674)

(22) 出願日 平成13年12月7日 (2001.12.7)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 石井 秀浩

東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(74) 代理人 100082131

弁理士 稲本 義雄

Fターム(参考) 5B085 AE23 AE29 BA07 BG03 BG07
5J104 AA09 AA13 AA16 PA07

(54) 【発明の名称】 情報処理装置および方法、プログラム格納媒体、並びにプログラム

(57) 【要約】

【課題】 コンテンツを自由に配布・流通させつつ、それを利用するためのライセンスを柔軟に設定できるようにする。

【解決手段】 コンテンツサーバは、クライアントにインターネットを介してコンテンツを提供するとき、コンテンツを暗号化する。その暗号化されたコンテンツのヘッダには、そのコンテンツに関する属性情報が記述される。クライアントは、コンテンツの属性情報が属性条件を満たすようなライセンスをライセンスサーバにアクセスして取得することで、暗号化されたコンテンツを許可するライセンスを取得する。

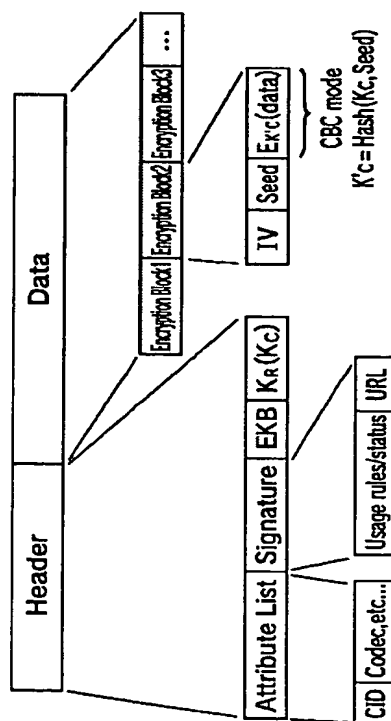


図5

【特許請求の範囲】

【請求項1】 暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信手段と、前記コンテンツを記憶するコンテンツ記憶手段と、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信手段と、前記ライセンスを記憶するライセンス記憶手段と、前記ライセンス記憶部に記憶されているライセンスが、前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすか否かを判定する判定手段と、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基いて、前記コンテンツの前記暗号化コンテンツデータを復号する復号手段と、前記復号手段により復号されたコンテンツデータを出力する出力手段と、を備えることを特徴とする情報処理装置。

【請求項2】 前記コンテンツは、更に前記コンテンツデータを復号するためのコンテンツキーを含む、ことを特徴とする請求項1記載の情報処理装置。

【請求項3】 前記属性情報は、属性項目と属性値の組み合わせからなる、ことを特徴とする請求項1記載の情報処理装置。

【請求項4】 前記属性項目はレコード会社、アーティスト、リリース日、コンテンツ発行者、ジャンル、サブスクリプション、またはレーベルに関する情報により規定される、ことを特徴とする請求項1記載の情報処理装置。

【請求項5】 前記属性条件は属性項目、属性値、及び演算子の組み合わせからなる、ことを特徴とする請求項1記載の情報処理装置。

【請求項6】 コンテンツに含まれる属性情報に関する条件を記載した属性条件を含むライセンスを一意に識別するライセンスIDを含むライセンス要求を受信する受信手段と、ライセンスをライセンスIDと共に記憶する記憶手段と、前記ライセンス要求に含まれる前記ライセンスIDに対応する前記ライセンスを取り込む取り込み手段と、前記ライセンスに電子署名を付加する署名手段と、署名手段により署名されたライセンスを送信する送信手段と、を備えることを特徴とする情報処理装置。

【請求項7】 更に、前記取り込み手段によって取り込まれたライセンスに端末IDを付加するライセンス処理手段、を備えることを特徴とする請求項6記載の情報処理装置。

【請求項8】 暗号化コンテンツデータと属性情報とを含むコンテンツを記憶する記憶手段と、コンテンツを一意に識別するコンテンツIDを含むコンテ

ンツ要求を受信する受信手段と、

コンテンツ要求に含まれるコンテンツIDに対応するコンテンツを送信する送信手段と、

を備える情報処理装置であって、

前記コンテンツに含まれる前記属性情報は、当該コンテンツを利用する際にライセンスの属性条件を満たすか否かを判断するために用いられる情報であり、前記ライセンスの属性条件は利用できる前記コンテンツの前記属性情報に関する条件を記載した情報である、ことを特徴とする情報処理装置。

【請求項9】 暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセンスを記憶するライセンス記憶ステップと、前記ライセンス記憶部に記憶されているライセンスが、前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすか否かを判定する判定ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基いて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップと、を含むことを特徴とする情報処理方法。

【請求項10】 暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセンスを記憶するライセンス記憶ステップと、前記ライセンス記憶部に記憶されているライセンスが、前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすか否かを判定する判定ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基いて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップと、をコンピュータに実行させるプログラム。

【請求項11】 暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記

載した属性条件を含むライセンスを受信するライセンス受信ステップと、

前記ライセンスを記憶するライセンス記憶ステップと、前記ライセンス記憶部に記憶されているライセンスが、前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすか否かを判定する判定ステップと、

前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、

前記復号手段により復号されたコンテンツデータを出力する出力ステップと、をコンピュータに実行させるプログラムが格納されたプログラム格納媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理装置および方法、プログラム格納媒体、並びにプログラムに関し、特に、著作権者からライセンスを受けていないコンテンツが不正にコピーされ、利用されるのを防止することができるようにした、情報処理装置および方法、プログラム格納媒体、並びにプログラムに関する。

【0002】

【従来の技術】最近、インターネットを介して、ユーザが、自分自身が保持している音楽データを他のユーザに提供し、自分自身が保持していない音楽データを他のユーザから提供を受けるようにして、複数のユーザが無料で音楽データを交換しあうシステムが実現されている。

【0003】このようなシステムでは、理論的には、1つの音楽、その他のコンテンツが存在すれば、他の全てのユーザが、それを利用することが可能となり、多くのユーザがコンテンツを購入しなくなるため、コンテンツに関する著作権者は、著作物としてのコンテンツが売れないため、著作物の販売に伴い、本来受け取ることが可能な著作物の利用に関するロイヤリティを受け取る機会を失うことになる。

【0004】そこで、配布されるコンテンツは暗号化しておき、そのコンテンツを利用するためのライセンスを別途発行し、暗号化されたコンテンツに対応するライセンスを持っていないとコンテンツを復号、再生できないようにするようにしたシステムがある。

【0005】このようにすることでコンテンツを自由に配布することを可能としつつ、著作物の著作権を保護することができる。

【0006】

【発明が解決しようとする課題】しかしながら、上記のシステムでは、ライセンスとコンテンツの対応関係を柔軟に設定したり、既に配布されたライセンスによって利用できるコンテンツを新たに配布することが難しかった。

【0007】本発明はこのような状況に鑑みてなされたものであり、コンテンツは自由に配布・流通させ、ライ

センスによって利用できるコンテンツの集合を自由に設定することができるようにするものである。

【0008】

【課題を解決するための手段】本発明の第1の情報処理装置は、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信手段と、前記コンテンツを記憶するコンテンツ記憶手段と、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信手段と、前記ライセンスを記憶するライセンス記憶手段と、前記ライセンス記憶部に記憶されているライセンスが、前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすか否かを判定する判定手段と、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基づいて、前記コンテンツの前記暗号化コンテンツデータを復号する復号手段と、前記復号手段により復号されたコンテンツデータを出力する出力手段とを備えることを特徴とする。

【0009】前記コンテンツは、更に前記コンテンツデータを復号するためのコンテンツキーを含むようにすることができる。

【0010】前記属性情報は、属性項目と属性値の組み合わせから構成することができる。

【0011】前記属性項目はレコード会社、アーティスト、リリース日、コンテンツ発行者、ジャンル、サブスクリプション、またはレーベルに関する情報により規定することができる。

【0012】前記属性条件は属性項目、属性値、及び演算子の組み合わせから構成することができる。

【0013】本発明の第2の情報処理装置は、コンテンツに含まれる属性情報に関する条件を記載した属性条件を含むライセンスを一意に識別するライセンスIDを含むライセンス要求を受信する受信手段と、ライセンスをライセンスIDと共に記憶する記憶手段と、前記ライセンス要求に含まれる前記ライセンスIDに対応する前記ライセンスを取り込む取り込み手段と、前記ライセンスに電子署名を付加する署名手段と、署名手段により署名されたライセンスを送信する送信手段とを備えることを特徴とする。

【0014】更に、前記取り込み手段によって取り込まれたライセンスに端末IDを付加するライセンス処理手段を備えることができる。

【0015】本発明の第3の情報処理装置は、暗号化コンテンツデータと属性情報とを含むコンテンツを記憶する記憶手段と、コンテンツを一意に識別するコンテンツIDを含むコンテンツ要求を受信する受信手段と、コンテンツ要求に含まれるコンテンツIDに対応するコンテンツを送信する送信手段とを備える情報処理装置であって、前記コンテンツに含まれる前記属性情報は、当該コンテンツを利用する際にライセンスの属性条件を満たすか否

かを判断するために用いられる情報であり、前記ライセンスの属性条件は利用できる前記コンテンツの前記属性情報に関する条件を記載した情報であることを特徴とする。

【0016】本発明の情報処理方法は、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセンスを記憶するライセンス記憶ステップと、前記ライセンス記憶部に記憶されているライセンスが、前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすか否かを判定する判定ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基いて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップとを含むことを特徴とする。

【0017】本発明のプログラムは、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセンスを記憶するライセンス記憶ステップと、前記ライセンス記憶部に記憶されているライセンスが、前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすか否かを判定する判定ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基いて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップとをコンピュータに実行させるプログラムである。

【0018】本発明のプログラム格納媒体に格納されているプログラムは、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセンスを記憶するライセンス記憶ステップと、前記ライセンス記憶部に記憶されているライセンスが、前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすか否かを判定する判定ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基いて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップ

とをコンピュータに実行させるプログラムである。

【0019】

【発明の実施の形態】図1は、本発明を適用したコンテンツ提供システムの構成を示している。インターネット2には、クライアント1-1、1-2（以下、これらのクライアントを個々に区別する必要がある場合、単にクライアント1と称する）が接続されている。この例においては、クライアントが2台のみ示されているが、インターネット2には、任意の台数のクライアントが接続される。

【0020】また、インターネット2には、クライアント1に対してコンテンツを提供するコンテンツサーバ3、コンテンツサーバ3が提供するコンテンツを利用するのに必要なライセンスをクライアント1に対して付与するライセンスサーバ4、およびクライアント1がライセンスを受け取った場合に、そのクライアント1に対して課金処理を行う課金サーバ5が接続されている。

【0021】これらのコンテンツサーバ3、ライセンスサーバ4、および課金サーバ5も、任意の台数、インターネット2に接続される。

【0022】図2はクライアント1の構成を表している。

【0023】図2において、CPU（Central Processing Unit）21は、ROM（Read Only Memory）22に記憶されているプログラム、または記憶部28からRAM（Random Access Memory）23にロードされたプログラムに従って各種の処理を実行する。タイマ20は、計時動作を行い、時刻情報をCPU21に供給する。RAM23にはまた、CPU21が各種の処理を実行する上において必要なデータなども適宜記憶される。

【0024】暗号化復号部24は、コンテンツデータを暗号化するとともに、既に暗号化されているコンテンツデータを復号する処理を行う。コーデック部25は、例えば、ATRAC（Adaptive Transform Acoustic Coding）3方式などでコンテンツデータをエンコードし、入出力インタフェース32を介してドライブ30に接続されている半導体メモリ44に供給し、記録させる。あるいはまた、コーデック部25は、ドライブ30を介して半導体メモリ44より読み出した、エンコードされているデータをデコードする。

【0025】半導体メモリ44は、例えば、メモリスティック（商標）などにより構成される。

【0026】CPU21、ROM22、RAM23、暗号化復号部24、およびコーデック部25は、バス31を介して相互に接続されている。このバス31にはまた、入出力インタフェース32も接続されている。

【0027】入出力インタフェース32には、キーボード、マウスなどよりなる入力部26、CRT、LCDなどよりなるディスプレイ、並びにスピーカなどよりなる出力部27、ハードディスクなどより構成される記憶部28、

モデム、ターミナルアダプタなどより構成される通信部29が接続されている。通信部29は、インターネット2を介しての通信処理を行う。通信部29はまた、他のクライアントとの間で、アナログ信号またはデジタル信号の通信処理を行う。

【0028】入出力インタフェース32にはまた、必要に応じてドライブ30が接続され、磁気ディスク41、光ディスク42、光磁気ディスク43、或いは半導体メモリ44などが適宜装着され、それらから読み出されたコンピュータプログラムが、必要に応じて記憶部28にインストールされる。

【0029】なお、図示は省略するが、コンテンツサーバ3、ライセンスサーバ4、課金サーバ5も、図2に示したクライアント1と基本的に同様の構成を有するコンピュータにより構成される。

【0030】次に、図3のフローチャートを参照して、クライアント1がコンテンツサーバ3からコンテンツの提供を受ける処理について説明する。

【0031】ユーザが、入力部26を操作することでコンテンツサーバ3に対するアクセスを指令すると、CPU21は、通信部29を制御し、インターネット2を介してコンテンツサーバ3にアクセスさせる。ステップS2において、ユーザが、入力部26を操作して、提供を受けるコンテンツを指定すると、CPU21は、この指定情報を受け取り、通信部29から、インターネット2を介してコンテンツサーバ3に、指定されたコンテンツを通知する。図4のフローチャートを参照して後述するように、この通知を受けたコンテンツサーバ3は、暗号化されたコンテンツデータを送信してくるので、ステップS3において、CPU21は、通信部29を介して、このコンテンツデータを受信すると、ステップS4において、その暗号化されているコンテンツデータを記憶部28を構成するハードディスクに供給し、記憶させる。

【0032】次に、図4のフローチャートを参照して、クライアント1の以上の処理に対応するコンテンツサーバ3のコンテンツ提供処理について説明する。なお、以下の説明において、図2のクライアント1の構成は、コンテンツサーバ3の構成としても引用する。

【0033】ステップS21において、コンテンツサーバ3のCPU21は、インターネット2から通信部29を介してクライアント1よりアクセスを受けるまで待機し、アクセスを受けたと判定したとき、ステップS22に進み、クライアント1から送信されてきたコンテンツを指定する情報を取り込む。このコンテンツを指定する情報は、クライアント1が、図3のステップS2において通知してきた情報である。

【0034】ステップS23において、コンテンツサーバ3のCPU21は、記憶部28に記憶されているコンテンツデータの中から、ステップS22の処理で取り込まれた情報で指定されたコンテンツを読み出す。CPU21

は、ステップS24において、記憶部28から読み出されたコンテンツデータを、暗号化復号部24に供給し、暗号化させる。

【0035】記憶部28に記憶されているコンテンツデータは、コーデック部25により、既にATRAC3方式によりエンコードされているので、このエンコードされているコンテンツデータが暗号化されることになる。

【0036】なお、もちろん、記憶部28に予め暗号化した状態でコンテンツデータを記憶させることができる。この場合には、ステップS24の処理は省略することが可能である。

【0037】次に、ステップS25において、コンテンツサーバ3のCPU21は、暗号化したコンテンツデータを伝送するフォーマットを構成するヘッダに、暗号化されているコンテンツを復号するのに必要なキーと、コンテンツに関する各種情報を示す属性情報を付加する。そして、ステップS26において、コンテンツサーバ3のCPU21は、ステップS24の処理で暗号化したコンテンツと、ステップS25の処理でキーと属性情報及びその電子署名を付加したヘッダとをフォーマット化したデータを、通信部29から、インターネット2を介して、アクセスしてきたクライアント1に送信する。

【0038】図5は、このようにして、コンテンツサーバ3からクライアント1にコンテンツが供給される場合のフォーマットの構成を表している。同図に示されるように、このフォーマットは、ヘッダ(Header)とデータ(Data)とにより構成される。

【0039】ヘッダには、属性情報(Attribute List)及び属性情報をライセンスサーバの暗号鍵で署名した電子署名、イネープリングキーブロック(EKB(Enabling KeyBlock))および、EKBをDNKを用いて復号処理することによって得られるルートキーKRIにより暗号化されたコンテンツキーKc(KR(Kc))が配置されている。

【0040】属性情報には属性項目と属性値との組み合わせからなる属性のエントリが複数記述されている。

【0041】属性項目の種類を図6に示す。CID、RCID、CIID、AID、GID及びLIDはそれぞれコンテンツ、レコード会社、コンテンツ発行者、アーティスト、ジャンル及びレーベルを一意に識別するIDである。RelDateはコンテンツのリリース日を表す。サブスクリプションIDは後述するサブスクリプションライセンスに用いられる属性項目である。

【0042】URLは、コンテンツを利用するためのライセンスを取得するときアクセスするアドレス情報であり、図1のシステムの場合、具体的には、ライセンスを受けるために必要なライセンスサーバ4のアドレスである。

【0043】データは、任意の数の暗号化ブロック(Encryption block)により構成される。各暗号化ブロックは、イニシャルベクトル(IV(Initial Vector))、シ

ード (Seed)、およびコンテンツデータをキー K' で暗号化したデータ $E_{K'}(data)$ により構成されている。

【0044】キー K' は、次式により示されるように、コンテンツキー K_c と、乱数で設定される値Seedをハッシュ関数に適用して演算された値により構成される。

【0045】 $K' = \text{Hash}(K_c, \text{Seed})$

【0046】イニシャルベクトルIVとシードSeedは、各暗号化ブロック毎に異なる値に設定される。

【0047】この暗号化は、コンテンツのデータを8バイト単位で区分して、8バイト毎に行われる。後段の8バイトの暗号化は、前段の8バイトの暗号化の結果を利用して行われるCBC (Cypher Block Chaining) モードで行われる。

【0048】CBCモードの場合、最初の8バイトのコンテンツデータを暗号化するとき、その前段の8バイトの暗号化結果が存在しないため、最初の8バイトのコンテンツデータを暗号化するときは、イニシャルベクトルIVを初期値として暗号化が行われる。

【0049】このCBCモードによる暗号化を行うことで、1つの暗号化ブロックが解読されたとしても、その影響が、他の暗号化ブロックにおよぶことが抑制される。

【0050】なお、この暗号化については、図14と図15を参照にして、後に詳述する。

【0051】以上のようにして、クライアント1は、コンテンツサーバ3からコンテンツを無料で、自由に取得することができる。

【0052】しかしながら、各クライアント1は、取得したコンテンツを利用するとき、ライセンスを取得する必要がある。

【0053】ライセンスを取得する際には、クライアント1は事前にライセンスサーバにオンラインあるいはオフラインで登録処理を行い、サービスデータを取得しておく。サービスデータにはデバイスノードキー (DNK) 及び端末IDが含まれており、EKBを復号処理するのに用いられる。サービスデータ及びライセンスサーバから取得するライセンスはクライアント1の記憶部28にセキュアに保存される。

【0054】図7にライセンスの構成を示す。ライセンスにはライセンスID、タイムスタンプ、使用期限、属性条件、使用規則、及びこれらをライセンスサーバの秘密鍵で署名した電子署名が含まれる。タイムスタンプはライセンスの発行日を表す。使用期限はライセンスを使用できる期限日を表し、この期限日を過ぎるとそのライセンスは使用できなくなる。属性条件はそのライセンスを所持しているクライアント1が利用できるコンテンツの属性の条件を属性項目と属性項目に関する値、比較演算子、及び論理演算子の組み合わせからなる条件式によって表したものである。使用規則にはそのライセンスの利用できるコンテンツを使用するための規則を記述したも

のであり、サービスデータに含まれているものと同じ端末IDが含まれる。

【0055】以下に、コンテンツに含まれる属性情報、及びライセンスに含まれる属性条件との組み合わせによって実現可能なライセンス構成の例を示す。

【0056】コンテンツ c_1 の属性情報には、次のように記述されている。

c_1 : $cid = \{1\}$, $aid = \{0, 1\}$, $reldate = 2000\text{年}11\text{月}10\text{日}$

【0057】これは、コンテンツIDは1、アーティストIDは0および1 (即ち、0番のアーティストと1番のアーティストの合作)、リリース日は2000年11月10日であるということを表す。

【0058】同様に、コンテンツ c_2 , c_3 , c_4 の属性情報に、次のように記述されている。

c_2 : $cid = \{2\}$, $aid = \{0\}$, $reldate = 2000\text{年}12\text{月}20\text{日}$

c_3 : $cid = \{3\}$, $aid = \{0\}$, $reldate = 2001\text{年}3\text{月}1\text{日}$

c_4 : $cid = \{4\}$, $aid = \{0\}$, $reldate = 2001\text{年}10\text{月}21\text{日}$
一方、ライセンス11の属性条件には、次のように記述されている。

$l1$: $cid \ni 1 \vee cid \ni 2$

【0059】これにより、利用権 r_1 はコンテンツ c_1 と c_2 に対応する。即ち、利用権 r_1 が有効な端末では、コンテンツ c_1 と c_2 を利用する事ができる。

【0060】ライセンス12の属性条件は、次のように記述されている。

$l2$: $aid \ni 0 \wedge (2001\text{年}1\text{月}1\text{日} < reldate < 2001\text{年}12\text{月}31\text{日})$

【0061】これは、2001年にリリースされた0番のアーティストのコンテンツ、という意味の条件であり、ライセンス12はコンテンツ c_3 と c_4 に対応する。この時点で、ライセンス12が有効な端末では、コンテンツ c_3 と c_4 を利用する事ができる。後に下記のような属性情報を持たせたコンテンツ c_5 が発行されたとする。

c_5 : $cid = \{5\}$, $aid = \{0\}$, $reldate = \{2001\text{年}12\text{月}1\text{日}\}$

【0062】このコンテンツをコンテンツサーバ3からダウンロードするなどして入手すると、既にライセンス12を保有しているクライアント1では、新たにライセンスサーバ等に接続する必要なく、コンテンツ c_5 も利用できるようになる。

【0063】これらのコンテンツの配布後、配信事業者が新たにベスト版としてコンテンツ c_1 , c_2 , c_5 を組み合わせで発売しようとするならば、それに対応する次のようなライセンス13を発行すれば、コンテンツを新たに作成する必要なく、配布済み・流通中のコンテンツをそのまま活用して、ベスト版発売が可能である。

$l3$: $cid \ni 1 \vee cid \ni 2 \vee cid \ni 5$

【0064】このようにして、配布済み・流通中のコンテンツを組み合わせた利用権を容易に新規発行できる。

例えば、リリース日とアーティストを制約した属性条件を持つライセンスを発行することで、1990年～1999年の谷村新司全集を新たに発売することができる。

【0065】また、アーティストを制約した属性条件を持つライセンスを発行することで、モーニング娘ファミリー全集（モーニング娘、プッチモニ、中澤裕子、他関連アーティストのコンテンツを集めたもの）を新たに発売することができる。

【0066】また、The Alfee Best（例えばコンテンツIDを制約する）。

【0067】次に、サブスクリプション・サービスとして、毎月いくつかの新譜を追加利用できるようになるライセンスを定義する例を示す。

【0068】ライセンス14の属性の条件を、次のように定義する。

14: cid \ni 3 \vee cid \ni 4 \vee sid \ni 1

【0069】このライセンス14を所持しているクライアント1では、まず、既に発行されているコンテンツc3とc4が利用可能である。翌月、新譜として次のような属性情報を持ったコンテンツc6とc7が発行されたとする。

c6: cid = {6}, sid = {1}

c7: cid = {7}, sid = {1}

【0070】この場合、ライセンス14を持っているクライアント1は、新たにライセンスを購入する必要なく、コンテンツc6とc7を利用する事ができる。同様に、月ごとにサブスクリプションIDに1を含んだコンテンツを発行する事により、ライセンス14を持っているクライアント1はライセンスを別途購入することなく、利用可能なコンテンツを追加していく事ができる。

【0071】このように、属性条件を属性項目、属性値、及び論理演算子、関係演算子等の演算子の組み合わせで表すことで、利用できるコンテンツの集合を柔軟に設定できるようになる。

【0072】属性条件に含まれる演算子はここに挙げられているに限定されず、その他の各種演算子を利用することができる。

【0073】図8を参照して、クライアント1がコンテンツを再生する場合の処理について説明する。

【0074】ステップS41において、クライアント1のCPU21は、ユーザが入力部26を操作することで指示したコンテンツIDを取得する。

【0075】そして、CPU21は、コンテンツIDを取得すると該当するコンテンツデータのヘッダに記述されている属性情報を読み取る。

【0076】次に、ステップS42に進み、CPU21は、ステップS41で読み取られた属性情報が各ライセンスに記述されている利用コンテンツ条件式を満たすライセンスが、クライアント1により既に取得され、記憶部28に記憶されているか否かを判定する。そのようなライセンスが見つからなかった場合には、ステップS4

3に進み、CPU21は、出力部27を介して、ディスプレイにライセンスの取得を促すメッセージを表示する。

【0077】ステップS42において、ライセンスが既に取得されていると判定された場合、ステップS44に進み、CPU21は、取得されているライセンスは有効期限内のものであるか否かを判定する。ライセンスが有効期限内のものであるか否かは、ライセンスの内容として規定されている期限と、タイマ20により計時されている現在日時と比較することがで判断される。ライセンスの有効期限が既に満了していると判定された場合、CPU21は、ステップS45に進み、ライセンス更新処理を実行する。このライセンス更新処理の詳細は、図8のフローチャートを参照して後述する。

【0078】ステップS44において、ライセンスはまだ有効期限内であると判定された場合、または、ステップS45において、ライセンスが更新された場合、ステップS45'に進み、CPU21は、コンテンツのヘッダに含まれる電子署名及びライセンスに含まれる電子署名をライセンスサーバ4の公開鍵で検証する。電子署名の検証の結果、電子署名が正しいと判断された場合、ステップS46に進み、CPU21は、暗号化されているコンテンツデータを記憶部28から読み出し、RAM23に格納させる。そして、ステップS47において、CPU21は、RAM23に記憶された暗号化ブロックのデータを、図5のデータに配置されている暗号化ブロック単位で、暗号化復号部24に供給し、復号させる。

【0079】CPU21は、さらに、ステップS48において、暗号化復号部24により復号されたコンテンツデータをコーデック部25に供給し、デコードさせる。そして、コーデック部25によりデコードされたデータを、CPU21は、入出力インタフェース32から出力部27に供給し、D/A変換させ、スピーカから出力させる。

【0080】図9～図11を用いてクライアントがライセンスサーバ4からライセンスを所得する処理を説明する。

【0081】図9はクライアント1のユーザが利用したいコンテンツが決まっている場合のライセンス取得処理を示している。ユーザが、入力部26を操作することでコンテンツを指定しライセンスサーバ4にライセンスリストの要求を指示すると、CPU21は、通信部29を制御し、インターネット2を介してコンテンツサーバ3に指定されたコンテンツのコンテンツIDを含むライセンスリスト要求を送信する。ライセンスサーバ4はライセンスリスト要求を受信すると、受信したライセンスリストに含まれるコンテンツIDから、該当するコンテンツを利用可能なライセンスを抽出し、各ライセンスのライセンスID、ライセンス名、利用できるコンテンツの条件、現在利用できるコンテンツのリスト、コンテンツの使用条

件等を記載したライセンスリストをクライアント1に送信する。

【0082】クライアント1がライセンスサーバ4からライセンスリストを受信すると、CPU21は、出力部27にライセンスリストに含まれる各ライセンスの情報を表示する。ユーザがその情報を参照し、所望するライセンスを選択すると、CPU21は、通信部29を制御し、SSLなどの相互認証によりセッションを形成した後、インターネット2を介してコンテンツサーバ3に、選択されたライセンスのライセンスIDと端末IDと課金用のユーザID及びパスワードを含むライセンス要求を暗号化して送信する。ライセンスサーバ4はクライアント1から送信されたライセンス要求を受信すると、後述するライセンス発行処理を行った後、ライセンス要求に含まれるライセンスIDに対応するライセンスをクライアント1に送信する。クライアント1はライセンスサーバ4から送信されたライセンスを受信すると、受信したライセンスを暗号化等をしてセキュアな状態で記憶部28に保存する。

【0083】以上のようにして、ユーザはクライアント1が既に所持しているコンテンツを利用するためのライセンスを取得することができる。以上のライセンス取得処理は、ユーザがクライアントに所持しているコンテンツを再生する操作した際に、そのコンテンツを再生するためのライセンスを取得していなかった場合、自動的に開始されるようにしても良い。

【0084】次に、ユーザが各種検索条件を指定してライセンスを検索し、取得する処理を図16に示す。まず、ユーザが欲しいライセンスを検索するための、ライセンス名、ライセンスの種類、ライセンスが利用可能とするコンテンツのタイトル、アルバム名、ジャンル、アーティスト名、リリース日等の検索条件を入力部26を操作することによって指定すると、CPU21は、通信部を制御し、入力された検索条件をフォーマットしたデータを含むライセンスリスト要求をコンテンツサーバ3に送信する。コンテンツサーバはクライアント1から送信されたライセンスリスト要求を受信すると、ライセンスリスト要求に含まれる検索条件を満たすライセンスを記憶部28から検索し、ライセンスID等の各ライセンスに関する情報を含むライセンスリストをクライアント1に送信する。

【0085】クライアント1がライセンスサーバ4からライセンスリストを受信すると、CPU21は、出力部27にライセンスリストに含まれる各ライセンスの情報を表示する。ユーザがその情報を参照し、所望するライセンスを選択すると、CPU21は、通信部29を制御し、SSLなどの相互認証によりセッションを形成した後、インターネット2を介してコンテンツサーバ3に、選択されたライセンスのライセンスIDと端末IDと課金用のユーザID及びパスワードを含むライセンス要求を暗号化して送信する。ライセンスサーバ4はクライアント1から送信

されたライセンス要求を受信すると、後述するライセンス発行処理を行った後、ライセンス要求に含まれるライセンスIDに対応するライセンスをクライアント1に送信する。クライアント1はライセンスサーバ4から送信されたライセンスを受信すると、受信したライセンスを暗号化するなどしてセキュアな状態で記憶部28に保存する。

【0086】以上のようにして、ユーザは欲しいライセンスを検索し、取得することができる。

【0087】次に、ユーザが欲しいライセンスのライセンスIDを知っている場合のライセンス取得処理を図11に示す。

【0088】ユーザがライセンスIDを入力部26を操作し入力して、欲しいライセンスのライセンスIDを指定すると、CPU21は、通信部29を制御し、SSLなどの相互認証によりセッションを形成した後、インターネット2を介してコンテンツサーバ3に、選択されたライセンスのライセンスIDと端末IDと課金用のユーザID及びパスワードを含むライセンス要求を暗号化して送信する。ライセンスサーバ4はクライアント1から送信されたライセンス要求を受信すると、後述するライセンス発行処理を行った後、ライセンス要求に含まれるライセンスIDに対応するライセンスをクライアント1に送信する。クライアント1はライセンスサーバ4から送信されたライセンスを受信すると、受信したライセンスを暗号化等をしてセキュアな状態で記憶部28に保存する。

【0089】以上のようにして、ユーザは雑誌などに記載されているライセンスの広告などからライセンスIDを知り、そのライセンスIDを指定することで所望するライセンスを取得することができる。

【0090】また、WebサイトのHTMLファイルや電子メール等にライセンスIDを含むライセンスサーバのURLのリンク情報が記載されており、これをユーザがクリックするなどして選択することでライセンス取得処理を開始するようにしても良い。

【0091】図12のフローチャートを参照して、で図9～図11におけるライセンス発行処理の詳細を説明する。なお、この場合においても、図2のクライアント1の構成は、ライセンスサーバ4の構成としても引用される。

【0092】最初にステップS102において、CPU21はライセンス要求に含まれるライセンスID、端末ID、ユーザID、パスワードを取り込む。

【0093】そして、ライセンスサーバ4のCPU21は、通信部29から課金サーバ5にアクセスし、ユーザIDとパスワードに対応するユーザの与信処理を要求する。課金サーバ5は、インターネット2を介してライセンスサーバ4から与信処理の要求を受けると、そのユーザIDとパスワードに対応するユーザの過去の支払い履歴などを調査し、そのユーザが、過去にライセンスの対価の不払いの実績があるか否かなどを調べ、そのような実

績がない場合には、ライセンスの付与を許容する与信結果を送信し、不払いの実績などがある場合には、ライセンス付与の不許可の与信結果を送信する。

【0094】ステップS104において、ライセンスサーバ4のCPU21は、課金サーバ5からの与信結果が、ライセンスを付与することを許容する与信結果であるかを判定し、ライセンスの付与が許容されている場合には、ステップS105に進み、ライセンスIDに対応するライセンスをデータベースから取り出し、ライセンスの使用規則のフィールドに端末IDを挿入し、ライセンスサーバ4の秘密鍵で電子署名を生成、付加する。

【0095】そして、ステップS107に進み、ライセンスサーバ4のCPU21は、その端末IDと電子署名が付加されたライセンスを通信部29からインターネット2を介してクライアント1に送信させる。

【0096】ステップS108においてライセンスサーバ4のCPU21は、ステップS107の処理で、いま送信したライセンスをステップS102の処理で取り込まれたユーザIDとパスワードに対応して、記憶部28に記憶させる。さらに、ステップS109において、CPU21は、課金処理を実行する。具体的には、CPU21は、通信部29から課金サーバ5に、そのユーザIDとパスワードに対応するユーザに対する課金処理を要求する。課金サーバ5は、この課金の要求に基づいて、そのユーザに対する課金処理を実行する。上述したように、この課金処理に対して、そのユーザが支払いを行わなかったような場合には、以後、そのユーザは、ライセンスの付与を要求したとしても、ライセンスを受けることができないことになる。

【0097】すなわち、この場合には、課金サーバ5からライセンスの付与を不許可とする与信結果が送信されてくるので、ステップS104からステップS110に進み、CPU21は、エラー処理を実行する。具体的には、ライセンスサーバ4のCPU21は、通信部29を制御してアクセスしてきたクライアント1に対して、ライセンスを付与することができない旨のメッセージを出力し、処理を終了させる。

【0098】この場合、上述したように、そのクライアント1はライセンスを受けることができないので、そのコンテンツを利用することができないことになる。

【0099】次に、図13を用いてライセンスが利用可能なコンテンツのコンテンツデータを取得する処理を説明する。

【0100】ユーザが入力部26を操作し、ライセンスを選択すると、CPUは、通信部29を制御し、インターネット2を介してコンテンツサーバ3に、選択されたライセンスのライセンスIDを含むコンテンツリスト要求を送信する。ライセンスサーバ4はコンテンツリスト要求を受信すると、コンテンツリスト要求に含まれるライセンスIDを取り出す。ライセンスサーバ4はライセンスID

をキーとしてライセンスデータベースから、該当するライセンスによって利用可能なコンテンツを抽出する。その後、ライセンスサーバは、抽出された各コンテンツのコンテンツID、コンテンツをダウンロードするためのURL、及びコンテンツ名、アーティスト名、ジャンル等のコンテンツ情報を含む、コンテンツリストをクライアント1に送信する。

【0101】クライアント1は出力部を制御してコンテンツリストを受信するとコンテンツリストに含まれる各コンテンツのコンテンツ情報を表示させる。ユーザが表示されたコンテンツ情報を参照して、ダウンロードするコンテンツを選択すると、クライアント1はコンテンツのURLに従って、コンテンツサーバにコンテンツ要求をコンテンツサーバ3に送信する。コンテンツサーバはコンテンツ要求を受信すると、コンテンツ要求に含まれるコンテンツIDを持つコンテンツをクライアント1に送信する。クライアント1はコンテンツサーバ3からコンテンツを受信すると、受信したコンテンツを記憶部28に記憶させる。

【0102】以上のようにして、ユーザはライセンスにより利用可能となるコンテンツを探し出し、コンテンツサーバ3からクライアントのダウンロードさせることができる。

【0103】図14は、ブロードキャストインクリプション (Broadcast Encryption) を、キーの管理方式に採用した場合におけるキーの構成方法を表している。図14に示されるように、キーは、階層ツリー構造とされ、最下段のリーフ (leaf) が個々のデバイスに対応する。図14の例の場合、番号0から番号15までの16個のデバイスに対応するキーが生成される。

【0104】各キーは、図中丸印で示される各ノードに対応して規定される。この例では、最上段のルートノードに対応してキーKRが、2番目のノードに対応してキーK0、K1が、3段目のノードに対応してキーK00乃至K11が、第4番目のノードに対応してキーK000乃至キーK111が、それぞれ対応されている。そして、最下段のノードとしてのリーフ (デバイスノード) に、キーK0000乃至K1111が、それぞれ対応されている。

【0105】階層構造とされているため、例えば、キーK0010とキー0011の上位のキーは、K001とされ、キーK000とキーK001の上位のキーは、K00とされている。以下同様に、キーK00とキーK01の上位のキーは、K0とされ、キーK0とキーK1の上位のキーは、KRとされている。

【0106】コンテンツを利用するために用いるキーは、最下段のデバイスノード (リーフ) から、最上段のルートノードまでの1つのパスの各ノードに対応するキーで構成される。例えば、番号3のコンテンツを利用するキーは、キーK0011、K001、K00、K0、

KRを含むパスの各キーで構成される。

【0107】本発明のシステムにおいては、例えば、図15に示されるように、 $8 \times 24 \times 32$ 段のノードに対応するキーで構成される階層ツリー構造キーシステムが利用される。このキーシステムでは、ルートノードから下位の8段までの各ノードに対応するキーに、カテゴリが対応される。ここにおけるカテゴリとは、例えばメモリスティックなどの半導体メモリを使用する機器のカテゴリ、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。

【0108】図15の例では、ルートノードから8段目のノードのうちの1つのノードに、本発明のシステムが対応される。このノードよりさらに下の階層の24段のノードに対応するキーにより、ライセンスが対応される。これにより、約16メガ(= 2^{24} = 約160万)のライセンスを規定することができる。さらに、最も下側の32段の階層により、約4ギガ(= 2^{32} = 約40億)のユーザを規定することができる。最下段の32段のノードに対応するキーが、DNK (Device Node Key) を構成する。

【0109】各コンテンツは、64(= $8 + 24 + 32$)段の各ノードで構成されるパスの内の1つに対応される。すなわち、各コンテンツの暗号化には、割り当てられたパスを構成するノードに対応するキーが用いられる。上位の階層のキーは、その直近の下位の階層のキーを用いて暗号化され、図5のEKB内に配置される。最下段のDNKは、EKB内には配置されず、クライアントがライセンスサーバに登録するときに取得するサービスデータに記述され、図16に示されるように、ユーザのクライアント1に与えられる。

【0110】クライアント1は、サービスデータに記述されているDNKを用いて、コンテンツデータとともに配布されるEKB内に記述されている直近の上位の階層のキーを復号し、復号して得たキーを用いて、EKB内に記述されているさらにその上の階層のキーを復号する。以上の処理を順次行うことで、クライアント1は、そのコンテンツのパスに属するすべてのキーを得ることができる。

【0111】クライアント1は以上のEKBの復号処理を行った後得られるKRを用いて、KRによって暗号化されているコンテンツキーKR(KC)を復号し、コンテンツキーKCを得ることができる。

【0112】なお、本発明におけるキーは、図14および図15に示されるようなブロードキャストインクリプションを利用したキーシステム以外のキーで構成することも可能である。

【0113】また、本発明が適用されるクライアントは、いわゆるパーソナルコンピュータ以外に、PDA (Personal Digital Assistants)、携帯電話機、ゲーム端末機などとしてすることができる。

【0114】一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

【0115】この記録媒体は、図2に示すように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク41 (フロッピディスクを含む)、光ディスク42 (CD-ROM (Compact Disk-Read Only Memory), DVD (Digital Versatile Disk) を含む)、光磁気ディスク43 (MD (Mini-Disk) を含む)、もしくは半導体メモリ44などよりなるパッケージメディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているROM22や、記憶部28に含まれるハードディスクなどで構成される。

【0116】なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0117】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0118】

【発明の効果】以上の如く、本発明の情報処理装置および方法、プログラム格納媒体、並びにプログラムによれば、暗号化されたデータとコンテンツの属性情報を、所定のフォーマットにフォーマット化して、出力するようにし、ライセンスに属性条件をふ含むようにし、コンテンツの属性情報がライセンスの属性条件を満たす場合に暗号化されたデータを復号できるようにしたので、データが不正に利用されるのを抑制しつつ、ライセンスを柔軟に発行することが可能となる。

【図面の簡単な説明】

【図1】本発明を適用したコンテンツ提供システムの構成を示すブロック図である。

【図2】図1のクライアントの構成を示すブロック図である。

【図3】図1のクライアントのコンテンツのダウンロード処理を説明するフローチャートである。

【図4】図1のコンテンツサーバのコンテンツ提供処理を説明するフローチャートである。

【図5】データフォーマットの例を示す図である。

【図6】属性項目の種類を説明する図である。

【図7】ライセンスの構成を示す図である。

【図8】クライアントの再生処理を説明するフローチャートである。

【図9】ライセンス取得処理を説明するフローチャートである。

【図10】ライセンス取得処理を説明するフローチャートである。

【図11】ライセンス取得処理を説明するフローチャートである。

【図12】ライセンス取得処理の詳細を説明するフローチャートである。

【図13】コンテンツデータを取得する処理を説明するフローチャートである。

【図14】キーの構成を説明する図である。

【図15】キーの構成とライセンスの関係を説明する図である。

【図16】ライセンスサーバのライセンス付与処理を説明する図である。

【符号の説明】

1-1, 1-2 クライアント, 2 インターネット, 3 コンテンツサーバ, 4 ライセンスサーバ, 5 課金サーバ, 20 タイマ, 21 CPU, 22 ROM, 23 RAM, 24 暗号化復号部, 25 コーデック部, 26 入力部, 27 出力部, 28 記憶部, 29 通信部

【図1】

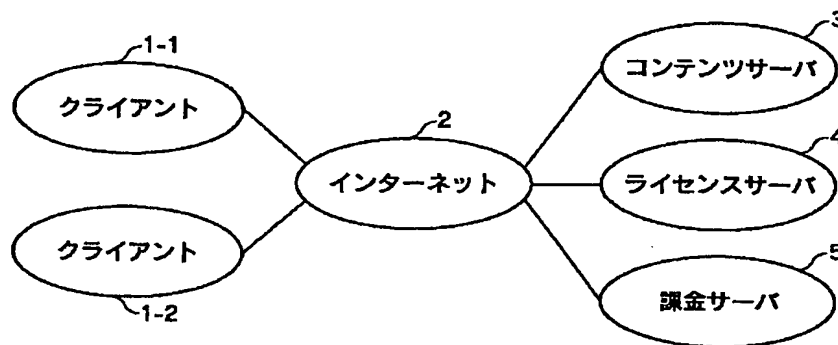


図1

【図3】

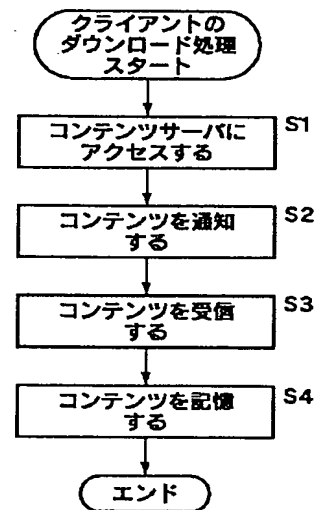


図3

【図2】

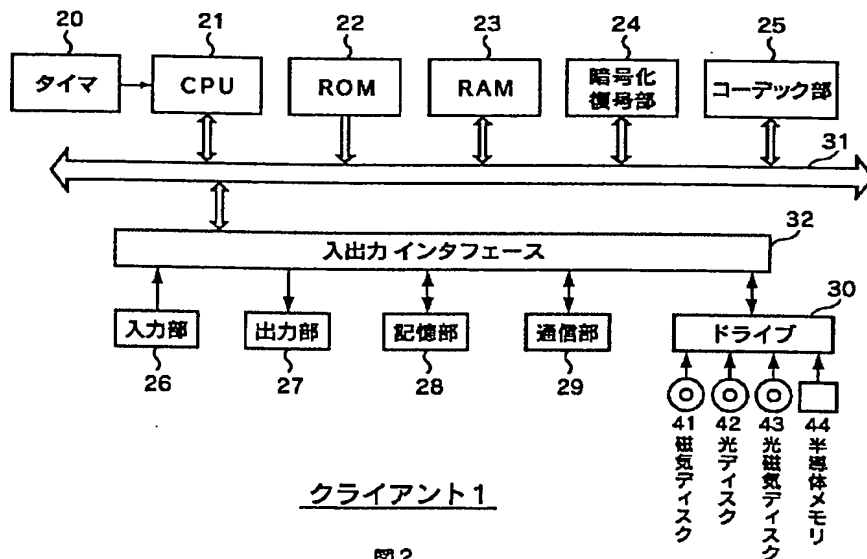


図2

【図7】

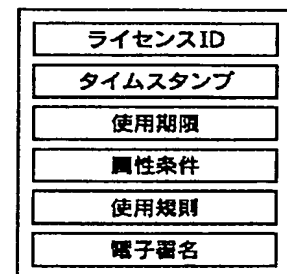


図7

【図4】

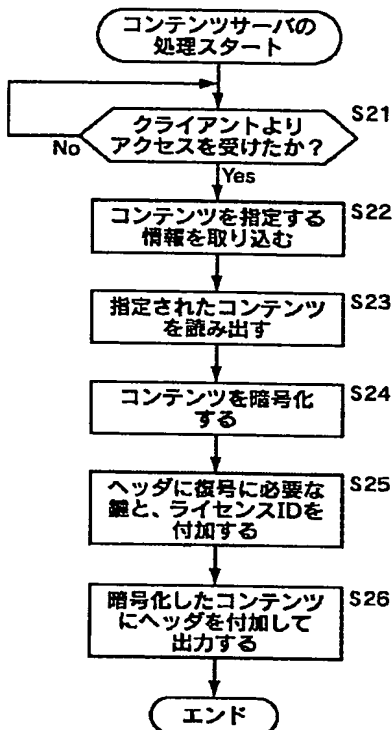


図4

【図6】

属性項目	説明
CID	コンテンツID
RCID	レコード会社ID
CIID	コンテンツ発行者ID
AID	アーティストID
RelDate	リリース日
GID	ジャンルID
LID	レーベルID
SID	サブスクリプションID
URL	ライセンスサーバのURL

図6

【図5】

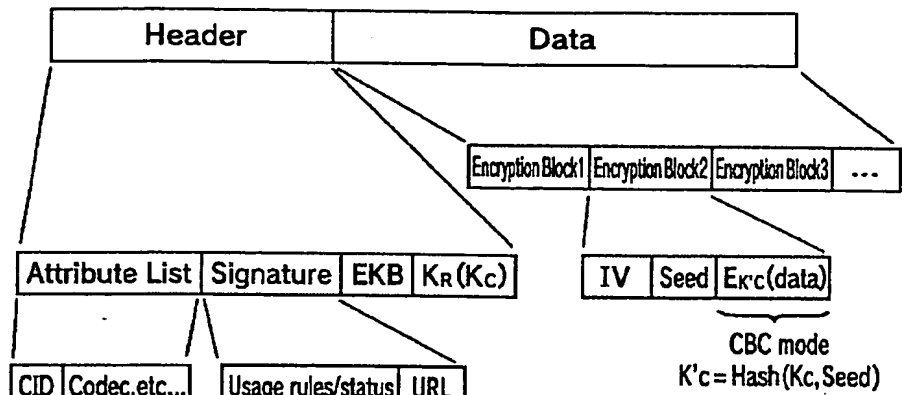


図5

【図8】

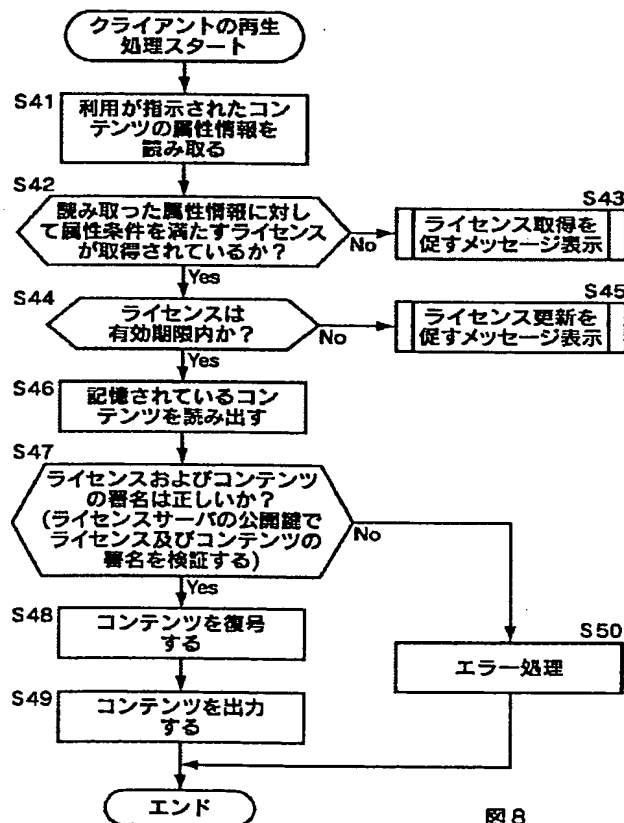


図8

【図 9】

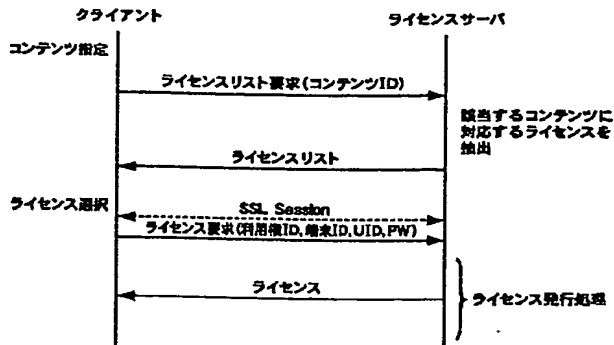


図 9

【図 10】

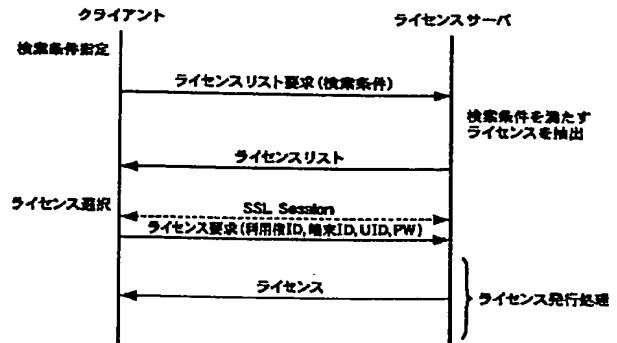


図 10

【図 11】

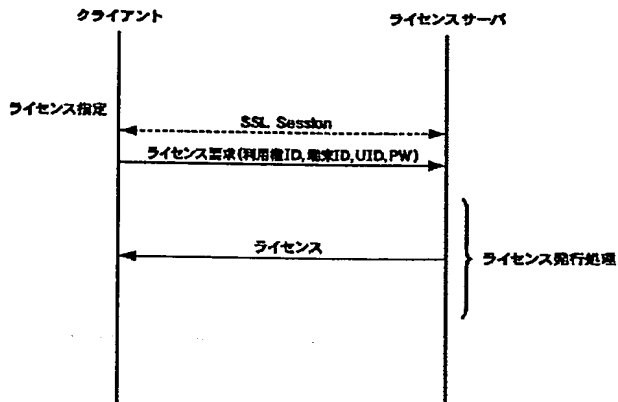


図 11

【図 12】

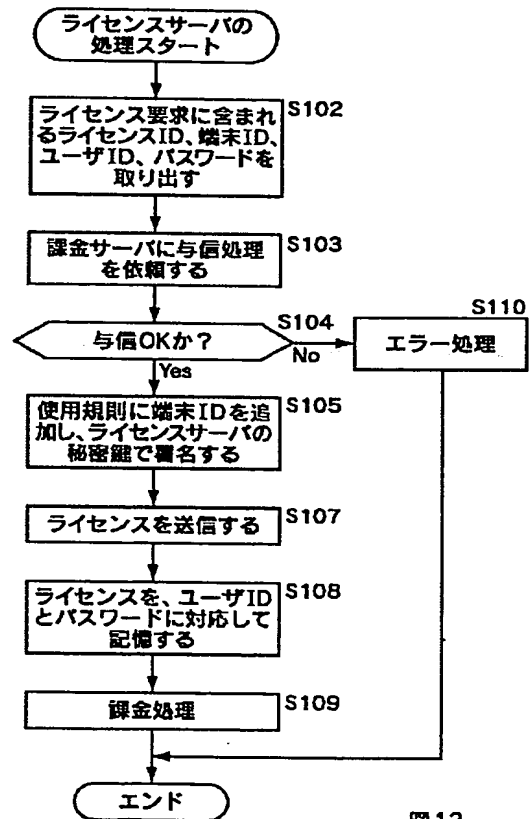


図 12

【図13】

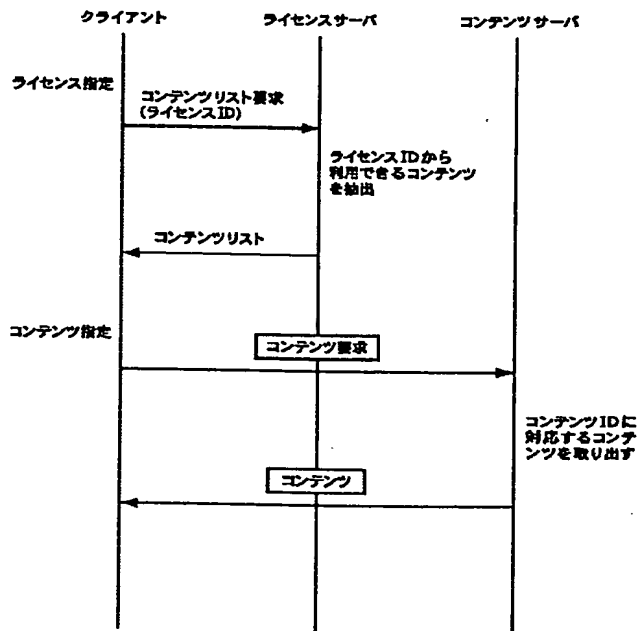


図13

【図15】

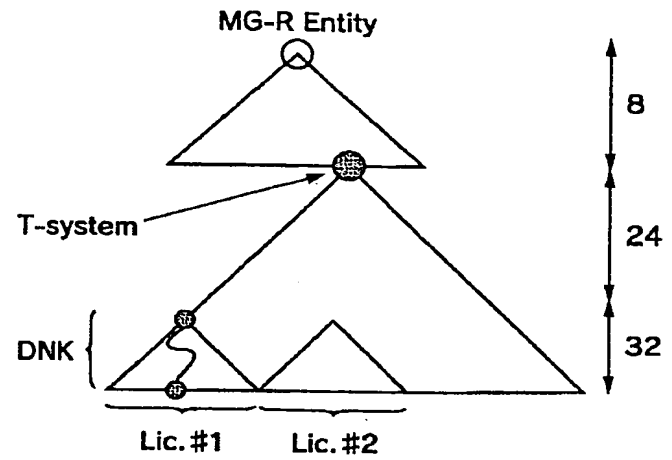


図15

【図14】

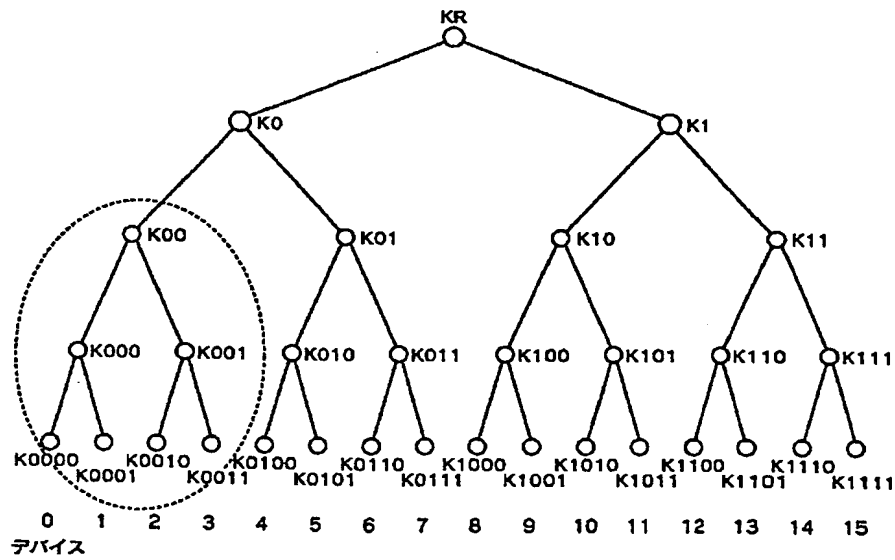


図14

【図16】

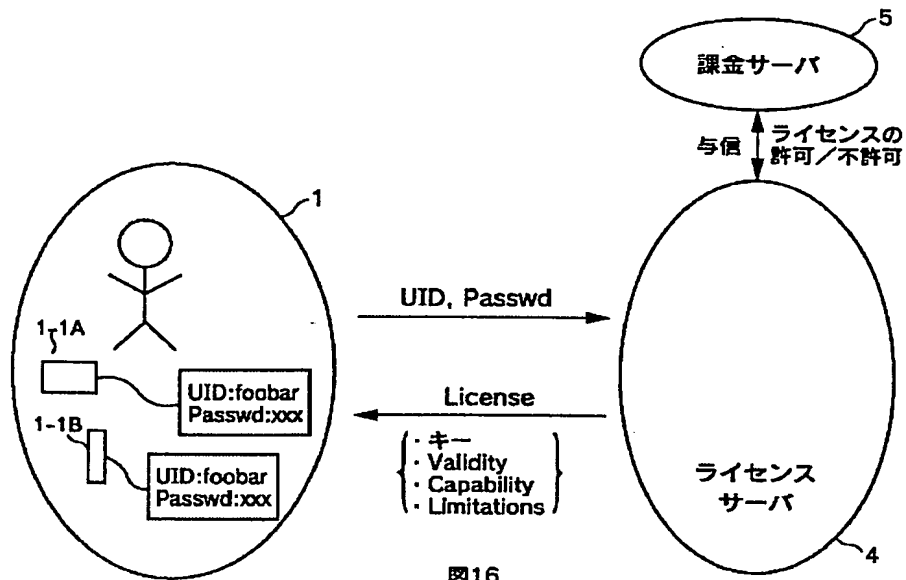


図16

【手続補正書】

【提出日】平成15年3月13日（2003. 3. 13）

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項1】 暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信手段と、前記コンテンツを記憶するコンテンツ記憶手段と、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信手段と、前記ライセンスを記憶するライセンス記憶手段と、前記コンテンツの前記属性情報が、前記ライセンス記憶手段に記憶されているライセンスの属性条件を満たすかを判定する判定手段と、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基いて、前記コンテンツの前記暗号化コンテンツデータを復号する復号手段と、前記復号手段により復号されたコンテンツデータを出力する出力手段とを備えることを特徴とする情報処理装置。

【請求項2】 前記コンテンツは、更に前記コンテンツデータを復号するためのコンテンツキーを含むことを特

徴とする請求項1に記載の情報処理装置。

【請求項3】 前記属性情報は、属性項目と属性値の組み合わせからなることを特徴とする請求項1に記載の情報処理装置。

【請求項4】 前記属性項目はレコード会社、アーティスト、リリース日、コンテンツ発行者、ジャンル、サブスクリプション、またはレーベルに関する情報を含むことを特徴とする請求項1に記載の情報処理装置。

【請求項5】 前記属性条件は属性項目、属性値、及び演算子の組み合わせからなることを特徴とする請求項1に記載の情報処理装置。

【請求項6】 コンテンツに含まれる属性情報に関する条件を記載した属性条件を含むライセンスを一意に識別するライセンスIDを含むライセンス要求を受信する受信手段と、

ライセンスをライセンスIDと共に記憶する記憶手段と、前記ライセンス要求に含まれる前記ライセンスIDに対応する前記ライセンスを取り込む取り込み手段と、前記ライセンスに電子署名を付加する署名手段と、署名手段により署名されたライセンスを送信する送信手段とを備えることを特徴とする情報処理装置。

【請求項7】 更に、前記取り込み手段によって取り込まれたライセンスに端末IDを付加するライセンス処理手段を備えることを特徴とする請求項6に記載の情報処理装置。

【請求項8】 暗号化コンテンツデータと属性情報とを含むコンテンツを記憶する記憶手段と、

コンテンツを一意に識別するコンテンツIDを含むコンテンツ要求を受信する受信手段と、
 コンテンツ要求に含まれるコンテンツIDに対応するコンテンツを送信する送信手段と、
 を備える情報処理装置であって、
 前記コンテンツに含まれる前記属性情報は、当該コンテンツを利用する際にライセンスの属性条件を満たすか否かを判断するために用いられる情報であり、
 前記ライセンスの属性条件は利用できる前記コンテンツの前記属性情報に関する条件を記載した情報であることを特徴とする情報処理装置。

【請求項 9】 暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、
 前記コンテンツを記憶するコンテンツ記憶ステップと、
 利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、
 前記ライセンスを記憶するライセンス記憶ステップと、
前記コンテンツの前記属性情報が、前記ライセンス記憶ステップの処理により記憶されたライセンスの属性条件を満たすか否かを判定する判定ステップと、
 前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基いて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、
 前記復号手段により復号されたコンテンツデータを出力する出力ステップとを含むことを特徴とする情報処理方法。

【請求項 10】 暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、
 前記コンテンツを記憶するコンテンツ記憶ステップと、
 利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、
 前記ライセンスを記憶するライセンス記憶ステップと、
前記コンテンツの前記属性情報が、前記ライセンス記憶ステップの処理により記憶されたライセンスの属性条件を満たすか否かを判定する判定ステップと、
 前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基いて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、
 前記復号手段により復号されたコンテンツデータを出力する出力ステップとをコンピュータに実行させるプログラム。

【請求項 11】 暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、
 前記コンテンツを記憶するコンテンツ記憶ステップと、

利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、
 前記ライセンスを記憶するライセンス記憶ステップと、
前記コンテンツの前記属性情報が、前記ライセンス記憶ステップの処理により記憶されたライセンスの属性条件を満たすか否かを判定する判定ステップと、
 前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基いて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、
 前記復号手段により復号されたコンテンツデータを出力する出力ステップとをコンピュータに実行させるプログラムが格納されたプログラム格納媒体。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】0008

【補正方法】変更

【補正内容】

【0008】

【課題を解決するための手段】本発明の第1の情報処理装置は、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信手段と、前記コンテンツを記憶するコンテンツ記憶手段と、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信手段と、前記ライセンスを記憶するライセンス記憶手段と、前記コンテンツの前記属性情報が、前記ライセンス記憶手段に記憶されているライセンスの属性条件を満たすか否かを判定する判定手段と、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基いて、前記コンテンツの前記暗号化コンテンツデータを復号する復号手段と、前記復号手段により復号されたコンテンツデータを出力する出力手段とを備えることを特徴とする。

【手続補正 3】

【補正対象書類名】明細書

【補正対象項目名】0011

【補正方法】変更

【補正内容】

【0011】前記属性項目はレコード会社、アーティスト、リリース日、コンテンツ発行者、ジャンル、サブスクリプション、またはレーベルに関する情報を含むようにすることができる。

【手続補正 4】

【補正対象書類名】明細書

【補正対象項目名】0016

【補正方法】変更

【補正内容】

【0016】本発明の情報処理方法は、暗号化コンテン

ッデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセンスを記憶するライセンス記憶ステップと、前記コンテンツの前記属性情報が、前記ライセンス記憶ステップの処理により記憶されたライセンスの属性条件を満たすか否かを判定する判定ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基ついて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップとを含むことを特徴とする。

【手続補正 5】

【補正対象書類名】明細書

【補正対象項目名】0017

【補正方法】変更

【補正内容】

【0017】本発明のプログラムは、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセンスを記憶するライセンス記憶ステップと、前記コンテンツの前記属性情報が、前記ライセンス記憶ステップの処理により記憶されたライセンスの属性条件を満たすか否かを判定する判定ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基ついて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップとをコンピュータに実行させるプログラムである。

【手続補正 6】

【補正対象書類名】明細書

【補正対象項目名】0018

【補正方法】変更

【補正内容】

【0018】本発明のプログラム格納媒体に格納されているプログラムは、暗号化コンテンツデータと属性情報とを含むコンテンツを受信するコンテンツ受信ステップと、前記コンテンツを記憶するコンテンツ記憶ステップと、利用できるコンテンツの前記属性情報に関する条件を記載した属性条件を含むライセンスを受信するライセンス受信ステップと、前記ライセンスを記憶するライセンス記憶ステップと、前記コンテンツの前記属性情報が、前記ライセンス記憶ステップの処理により記憶されたライセンスの属性条件を満たすか否かを判定する判定

ステップと、前記判定手段が前記コンテンツの前記属性情報が当該ライセンスの属性条件を満たすと判定したことに基ついて、前記コンテンツの前記暗号化コンテンツデータを復号する復号ステップと、前記復号手段により復号されたコンテンツデータを出力する出力ステップとをコンピュータに実行させるプログラムである。

【手続補正 7】

【補正対象書類名】明細書

【補正対象項目名】0078

【補正方法】変更

【補正内容】

【0078】ステップS44において、ライセンスはまだ有効期限内であると判定された場合、または、ステップS45において、ライセンスが更新された場合、ステップS45に進み、CPU21は、コンテンツのヘッダに含まれる電子署名及びライセンスに含まれる電子署名をライセンスサーバ4の公開鍵で検証する。電子署名の検証の結果、電子署名が正しいと判断された場合、ステップS46に進み、CPU21は、暗号化されているコンテンツデータを記憶部28から読み出し、RAM23に格納させる。そして、ステップS47において、CPU21は、RAM23に記憶された暗号化ブロックのデータを、図5のデータに配置されている暗号化ブロック単位で、暗号化復号部24に供給し、復号させる。

【手続補正 8】

【補正対象書類名】明細書

【補正対象項目名】0080

【補正方法】変更

【補正内容】

【0080】図9乃至図11を用いてクライアントがライセンスサーバ4からライセンスを取得する処理を説明する。

【手続補正 9】

【補正対象書類名】明細書

【補正対象項目名】0091

【補正方法】変更

【補正内容】

【0091】図12のフローチャートを参照して、図9乃至図11におけるライセンス発行処理の詳細を説明する。なお、この場合においても、図2のクライアント1の構成は、ライセンスサーバ4の構成としても引用される。

【手続補正 10】

【補正対象書類名】明細書

【補正対象項目名】0108

【補正方法】変更

【補正内容】

【0108】図15の例では、ルートノードから8段目のノードのうちの1つのノードに、本発明のシステムが対応される。このノードよりさらに下の階層の24段の

ノードに対応するキーにより、ライセンスが対応される。これにより、約16メガ(= 2^{24} = 約160万)のライセンスを規定することができる。さらに、最も下側の32段の階層により、約4ギガ(= 2^{32} = 約40億)のユーザを規定することができる。最下段の32段のノードに対応するキーが、DNK (Device Node Key) を構成する。

【手続補正11】

【補正対象書類名】図面

【補正対象項目名】図4

【補正方法】変更

【補正内容】

【図4】

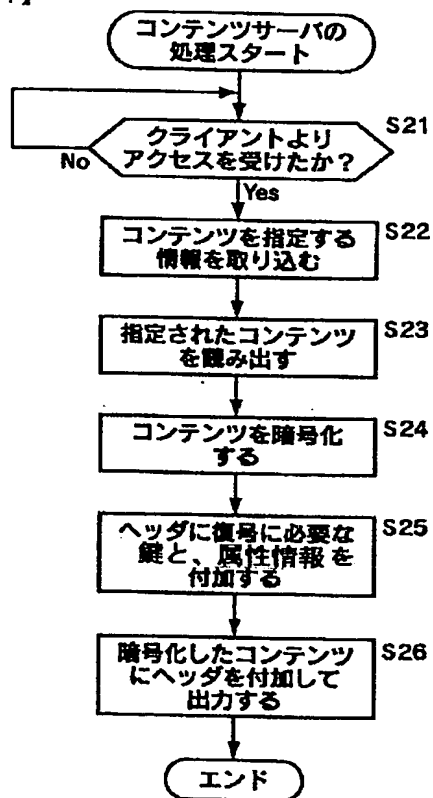


図4